UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

PHILLIP GERVAIS,

individually and on behalf of all others similarly situated,

Plaintiff,

v.

LUXOTTICA OF AMERICA INC.,

Defendant.

Case No. 1:20-cv-983

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff Phillip Gervais ("Plaintiff"), individually and on behalf of all other persons similarly situated, and through his attorneys of record, alleges the following against Defendant Luxottica of America Inc. ("Luxottica" or "Defendant") based upon personal knowledge with respect to himself, on information and belief derived from investigation by his counsel, and review of public documents as to all other matters.

INTRODUCTION

1. Luxottica is the service provider to Plaintiff's eye healthcare provider, Target Optical. Target Optical utilizes Luxottica's online eye doctor appointment scheduling application (the "Scheduling Application"), which is used by its patients to schedule appointments online or over the phone.[1] Plaintiff has been a patient at Target Optical since May 2018 and has made various appointments through the Scheduling Application. Unfortunately for Plaintiff, Luxottica did not adequately safeguard his data, and he and thousands of other patients are now the victims of a large-scale, long-lasting data breach that will impact them for years to come.

2. Luxottica is responsible for allowing the data breach to occur because it failed to implement and maintain reasonable safeguards and failed to comply with industry-standard data security practices, contrary to the representations made in its Privacy Policy and incorporated HIPAA Notice.

3. During the duration of the data breach, Luxottica failed to detect unauthorized third parties' access to its computer data and storage systems, notice the massive amounts of data that were compromised, and failed to take any steps to investigate the red flags that should have warned Luxottica that its systems were not secure.

4. Luxottica had obligations created by HIPAA, contract, industry standards, common law, and representations made to Plaintiff and class members, to keep their personal identifiable information ("PII"), including protected health information ("PHI"), confidential and to protect it from unauthorized access and disclosure.

[1] https://securityaffairs.co/wordpress/110565/data-breach/luxottica-lenscrafters-eyemed-data-breach.html (last visited November 21, 2020).

5. Plaintiff and class members provided their PII to Luxottica with the reasonable expectation and mutual understanding that Luxottica would comply with its obligations to keep such information confidential and secure from unauthorized access.

6. Luxottica's data security obligations were particularly important given the substantial increase in cyberattacks and data breaches in the healthcare industry preceding the date of the data breach.

7. As a result of Luxottica's failure to protect the consumer information it was entrusted with, Plaintiff and class members have been exposed to and/or are at a significant risk of identity theft, financial fraud, and other identity-related fraud into the indefinite future. Plaintiff and class members have also lost the inherent value of their PII. This harm was compounded by Luxottica's failure to ensure that patients of its eye healthcare providers received proper and timely notification of the data breach.

PARTIES

8. Plaintiff is a citizen and resident of the State of California. Plaintiff made an appointment and received eye healthcare treatment from Target Optical, one of Luxottica's eye healthcare providers. He entrusted PII, including PHI, to Luxottica with the reasonable expectation and understanding that Luxottica would protect and safeguard that information from compromise, disclosure, and misuse by unauthorized users, and would be timely notified of any data security incidents involving his PII should such occur.

9. Luxottica is an Ohio corporation with its principal place of business in Mason, Ohio. It is the subsidiary of Luxottica Group S.p.A., an Italian eyewear conglomerate. Luxottica was formerly known as Luxottica Retail North America Inc.

10. Luxottica produces and licenses eyewear under numerous brand names, including Coach, Chanel, Dolce & Gabbana, Oakley, Prada, and Ray-Ban, among others.[2] It also operates various retail brands, including LensCrafters, Pearle Vision, Sunglass Hut, and Target Optical.[3] In

[2] http://www.luxottica.com/en/eyewear-brands (last visited November 21, 2020).
[3] http://www.luxottica.com/en/retail-brands (last visited November 21, 2020).

addition, Luxottica operates EyeMed Vision Care, "the second largest vision benefits company in the United States, serving approximately 52 million members in large, medium and small-sized companies, as well as government entities."[4]

11. Luxottica provides optometry and vision services to customers in connection with some of its retail operations (*i.e.*, eye healthcare providers), including Target Optical. In the ordinary course of receiving treatment and heath care services from Luxottica, optometry and vision service customers ("Patients") are required to provide contact information (including, but not limited to, name, email, and shipping address) and financial information (including, but not limited to, credit card number, expiration date, etc.).[5] Patients also must provide their date of birth, insurance information and coverage, and other information that may be deemed necessary to provide care.

12. Luxottica also gathers certain medical information about Patients and creates records of the care it provides them.

13. Additionally, Luxottica may receive private and personal information from other individuals and/or organizations that are part of a Patient's "circle of care," such as referring physicians, Patients' other doctors, Patients' plan(s), close friends, and/or family members.

14. All of Luxottica's current and future affiliates and other brands may share Patient information with each other for various purposes.[6]

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than 100 putative class members, and minimal diversity exists because putative class members are citizens of a different state than Luxottica.

---

[4] http://www.luxottica.com/en/retail-brands/eyemed-vision-care (last visited November 21, 2020).
[5] https://web.archive.org/web/20171206105128/http://www.targetoptical.com/to-us/privacy-policy#privacyStatement (last visited November 24, 2020).
[6] *Id.*

16. This Court has personal jurisdiction over Luxottica because it is authorized to and regularly conducts business in Ohio and is headquartered in Mason, Ohio.

17. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

Luxottica and Its Privacy and Data Security Representations

18. Luxottica touts that it is "a market leader in the design, manufacture and distribution of fashion, luxury, sports and performance eyewear."[7] As of December 31, 2019, Luxottica operated a total of 3,849 corporate stores in North America, including multiple Target Optical locations throughout the United States.[8]

19. Luxottica's EyeMed Vision Care is the second largest vision benefits company in the United States, serving over 52,000,000 members.[9]

20. Luxottica is fully aware of the sensitive nature of Patients' PII and PHI stored on or processed through its systems.

21. Luxottica's Privacy Policy states that it collects certain PII from consumers, including: (1) contact information (including, but not limited to, name, email, and shipping address); and (2) financial information (including, but not limited to, credit card number, expiration date, etc.).[10] The Privacy Policy is provided to every Patient upon request and is posted on Luxottica's websites.

---

[7] http://www.luxottica.com/en (last visited November 21, 2020).

[8] https://www.statista.com/statistics/241663/number-of-stores-of-luxottica-in-north-america/#:~:text=As%20of%20December%2031%2C%202019,corporate%20stores%20in%20North%20America (last visited November 21, 2020); https://local.targetoptical.com/ (last visited November 24, 2020).

[9] www.luxottica.com/sites/luxottica.com/files/luxottica_group_relazione_finanziaria_annuale_2018_eng_20190410.pdf (last visited November 21, 2020).

[10] https://web.archive.org/web/20171206105128/http:/www.targetoptical.com/to-us/privacy-policy#privacyStatement (last visited November 24, 2020).

22. Luxottica makes representations to its customers and their Patients regarding its data security practices. Its Privacy Policy specifically states: "We follow generally accepted industry standards to protect the personal information submitted to us, both during transmission and once we receive it."[11]

23. In the course of treating Patients, Luxottica acquires, collects, and stores a massive amount of PII, including PHI, on its Patients.

24. As a condition of receiving healthcare services from Luxottica, Luxottica requires that its Patients entrust it with highly sensitive PII, including PHI.

25. Luxottica's HIPAA Notice provides that it collects PHI from Patients "for treatment, to obtain payment for treatment, for administrative purposes, and to evaluate the quality of care and service that you receive."[12] It further provides that, "[y]our health information is contained in a medical or optical dispensary record that is the physical property of Luxottica Retail.[13] Your health information consists of any information, whether in oral or recorded form, that is created or received by us and individually identifies you, and that relates to your past, present or future physical or mental health or condition; the provision of health care to you; or the past, present or future payment for the provision of health care to you."[14]

26. Recognizing the sensitivity of the health information it maintains, Luxottica has a HIPAA Notice stating that it is "committed to protecting your privacy," and that it is "required by applicable federal and state law to…[m]aintain the privacy and safeguard the security of your health information; [and] notify you, along with all other affected individuals, of a breach of unsecured health information…."[15]

---

[11] *Id.*
[12] https://web.archive.org/web/20170619102139/http://www.targetoptical.com/to-us/content/hipaa (last visited November 24, 2020).
[13] Luxottica is formerly known as Luxottica Retail North America Inc.
[14] *Id.*
[15] *Id.*

27. Luxottica's HIPAA Notice specifically sets forth expectations for Luxottica's behavior in the event of a data breach, providing that if Luxottica "discover[s] that your health information has been breached (for example, disclosed to or acquired by an unauthorized person, stolen, lost, or otherwise used or disclosed in violation of applicable privacy law) and the privacy or security of the information has been compromised, we must notify you of the breach without unreasonable delay and in no event later than 60 days following our discovery of the breach."

28. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and class member's PII, Luxottica assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff and class members' PII from disclosure.

29. Plaintiff and class members have taken reasonable steps to maintain the confidentiality of their PII.

30. Plaintiff and class members relied on Luxottica to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Luxottica's Knowledge That It Was and Is a Target of Cyber Threats

31. Luxottica knew it was a prime target for hackers given the significant amount of sensitive Patient PII processed through its computer data and storage systems.

32. Experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

33. Luxottica's knowledge is underscored by the massive number of data breaches, including those perpetrated against the healthcare sector, that have occurred in recent years. Over 41 million patient records were breached in 2019, with a single hacking incident affecting close to 21 million records.[16] Healthcare data breaches in 2019 almost tripled those the healthcare industry

[16] https://www.fiercehealthcare.com/tech/number-patient-records-breached-2019-almost-tripled-from-2018-as-healthcare-faces-new-threats (last visited November 25, 2020).

experienced in 2018 when 15 million patient records were affected by breach incidents, according to a report from Protenus and DataBreaches.net.[17]

34. Protenus, a healthcare compliance analytics firm, analyzed data breach incidents disclosed to the U.S. Department of Health and Human Services or the media during 2019, finding there has been an alarming increase in the number of breaches of patient privacy since 2016, when there were 450 security incidents involving patient data.[18] In 2019, that number jumped to 572 incidents, which is likely an underestimate, as two of the incidents for which there were no data affected 500 dental practices and clinics and could affect significant volumes of patient records. There continues to be at least one health data breach per day.[19]

35. Despite knowing the prevalence of these healthcare data breaches, Luxottica failed to prioritize data security by adopting reasonable data security measures to prevent and detect unauthorized access to their highly sensitive systems and databases. Luxottica had the resources to prevent a breach, but neglected to adequately invest in data security, despite the growing number of well-publicized data breaches affecting the healthcare industry.

36. Luxottica failed to undertake adequate analyses and testing of its own systems, training of its own personnel, and other data security measures to ensure that similar vulnerabilities were avoided or remedied and that Plaintiff's and class members' PII and PHI was protected.

The Data Breach

37. On August 9, 2020, Luxottica allegedly learned that on August 5, 2020, an unauthorized person accessed the Scheduling Application (the "Data Breach"). According to Luxottica, upon learning of the Data Breach, it "contained it, and immediately began an investigation to determine the extent of the incident." On August 28, 2020, Luxottica preliminarily concluded that the attacker might have accessed and acquired patient information.[20]

---

[17] *Id.*; *see also* https://www.protenus.com/resources/2020-breach-barometer/ (last visited November 25, 2020).
[18] *Id.*
[19] *Id.*
[20] *https://luxottica.kroll.com/*(last visited November 21, 2020).

38. Despite having knowledge of the Data Breach no later than August 2020, Luxottica did not issue a "Security Incident" notification until October 28, 2020, nor did it notify impacted patients until October 28, 2020 or later.[21]

39. The Security Incident notification disclosed that the personal information accessed in the Data Breach may have included: "full name, contact information, appointment date and time, health insurance policy number, and doctor or appointment notes that may indicate information related to eye care treatment, such as prescriptions, health conditions or procedures."[22]

40. Luxottica reported to the U.S. Department of Health and Human Services that the Data Breach compromised the PII of at least 829,454 Patients.[23]

41. On or about October 28, 2020, Plaintiff received a letter from Luxottica, disclosing that patient information may have been accessed or acquired by an attacker and that based on its investigation, it had determined that the personal information involved in the incident may have included Plaintiff's: "full name, contact information, appointment date and time, and doctor or appointment notes that may indicate information related to eye care treatment, such as prescriptions, health conditions, or procedures." A true and correct copy of the October 28, 2020 letter is attached hereto as **Exhibit A**.

42. Prior to receiving this letter, Plaintiff visited a Target Optical store in Santa Clara, California, on five to ten occasions from May 25, 2018 through November 19, 2020. At his October 3, 2020 visit, immediately preceding the Data Breach, Plaintiff obtained an annual vision exam, and purchased new prescription contacts. Plaintiff pays out-of-pocket copays for the services he receives from Target Optical.

43. Plaintiff provided his vision insurance information and, to the best of his recollection, information pertaining to his medical history to Luxottica or its employees in connection with his visits to Target Optical.

---

[21] *Id.*
[22] *Id.*
[23] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited November 30, 2020).

44. While Luxottica claimed it was "not aware of any misuse of personal information or harm to patients as a result of this incident," it could not rule out the possibility and advised Plaintiff to "remain vigilant, including by regularly reviewing your account statements."[24]

45. Moreover, the Data Breach follows a ransomware cyberattack in September 2020, involving Luxottica's parent company, Luxottica Group S.p.A., in which "some of the web sites operated by the company were not reachable, including Ray-Ban, Sunglass Hut, LensCrafters, EyeMed, and Pearle Vision."[25]

46. Thereafter, a "huge trove of files" was posted on the dark web, "related to the personnel office and finance departments," of Luxottica S.p.A.[26]

47. Cybersecurity intelligence firm Bad Packets posited that the source of the ransomware attack was "a Citrix ADX controller device vulnerable to the critical CVE-2019 19781 flaw."[27]

48. As a result, Luxottica and its international parent company have apparently suffered two serious data breaches in a span of only two months, signaling pervasive problems in Luxottica's cybersecurity practices.

49. Because of the nature of the PII stored or processed by Luxottica, Plaintiff understands that all categories of PII were subject to unauthorized access and exfiltration, theft, or disclosure. In other words, criminals would have no purpose for hacking Luxottica other than to exfiltrate or steal the coveted PII stored or processed by Luxottica.

50. Moreover, and notwithstanding the representations in its HIPAA Notice that it would notify affected individuals of a data breach without unreasonable delay and in no event later

---

[24] *See* Ex. A.

[25] https://securityaffairs.co/wordpress/108611/cyber-crime/luxottica-cyber-attack.html (last visited November 25, 2020).

[26] https://securityaffairs.co/wordpress/109778/data-breach/luxottica-data-leak-ransomware.html (last visited November 25, 2020); *see also* https://www.itwire.com/security/eyewear-giant-luxottica-hit-by-windows-nefilim-ransomware,-data-leaked.html (last visited November 25, 2020).

[27] https://www.bleepingcomputer.com/news/security/ray-ban-owner-luxottica-confirms-ransomware-attack-work-disrupted/ (last visited November 25, 2020).

than 60 days following discovery of the breach, Plaintiff did not receive notice of the Data Breach until October 28, 2020, more than 60 days following Luxottica's alleged discovery of the Data Breach.

51. Luxottica's response to the Data Breach caused confusion among the victims of the Data Breach, resulting in class members spending time, and continuing to spend a significant amount of time into the future, taking measures to protect themselves from identity theft, fraud, and other identity-related crimes.

52. Luxottica is responsible for allowing the Data Breach to occur because it failed to implement and maintain any reasonable safeguards and failed to comply with industry-standard data security practices, contrary to the representations made in Luxottica's Privacy Policy and HIPAA Notice and its explicit and implied agreements with its Patients, including Plaintiff and class members.

53. As a result of Luxottica's failure to protect the sensitive PII it was entrusted with, Plaintiff and class members are at a significant risk of identity theft, financial fraud, and other identity-related fraud into the indefinite future. Plaintiff and class members have also lost the inherent value of their PII.

54. Plaintiff and class members provided their PII to Luxottica with the expectation and understanding that Luxottica would adequately protect and store his data. If Plaintiff and class members had known that Luxottica's data security was insufficient to protect their PII, they would have demanded that their eye healthcare provider not store or process their PII through Luxottica's computer data and storage systems.

Luxottica Failed to Comply with Regulatory Guidance and Meet Consumers' Expectations

55. Federal agencies have issued recommendations and guidelines to temper data breaches and the resulting harm to individuals and financial institutions. For example, the FTC has issued numerous guides for business highlighting the importance of reasonable data security

practices. According to the FTC, the need for data security should be factored into all business decision-making.[28]

56. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[29] Among other things, the guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[30]

57. Additionally, the FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[31]

58. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C.

---

[28]Federal Trade Commission, *Start With Security* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited May 26, 2020).

[29]Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[30] *Id.*

[31]FTC, *Start With Security*, *supra* note 27.

§ 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[32]

59. In this case, Luxottica was fully aware of its obligation to use reasonable measures to protect the PII of its customers, acknowledging as much in its own Privacy Policy and HIPAA Notice. Luxottica also knew it was a target for hackers. But despite understanding the consequences of inadequate data security, Luxottica failed to comply with industry-standard data security requirements.

60. Luxottica's failure to employ reasonable and appropriate measures to protect against unauthorized access to Patients' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45, and various state consumer protection and data breach statutes.

Effect of the Data Breach

61. Luxottica's failure to keep Plaintiff and class members' PII secure has severe ramifications. Given the sensitive nature of the PII stolen in the Data Breach, cyber criminals have the ability to commit identity theft and other identity-related fraud against Plaintiff and class members now and into the indefinite future.

62. The information stolen from Luxottica included PHI, which "can fetch up to $350 on the dark web."[33] Stolen PHI is a one of the most valuable commodities on the criminal information black market. In 2014, the FBI warned healthcare organizations that PHI data is worth 10 times the amount of personal credit card data on the black market.[34] PHI data for sale is so

[32]Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited November 25, 2020).

[33] *How Cybercriminals Make Money: How much is your information worth to a cybercriminal via the Dark Web?*, Keeper Security, https://www.keepersecurity.com/how-much-is-my-information-worth-to-hacker-dark-web.html (last visited November 25, 2020).

[34] Stolen PHI health credentials can sell for up to 20 times the value of a U.S. credit card number, according to Don Jackson, director of threat intelligence at PhishLabs, a cyber-crime protection company who obtained this data by monitoring underground exchanges where cyber-criminals sell the information. *See* https://hipaahealthlaw.foxrothschild.com/2015/03/articles/articles/hacked-health-records-prized-for-their-black-market-

valuable because PHI information is so broad, and it can therefore be used for a wide variety of criminal activity such as to create fake IDs, buy medical equipment and drugs that can be resold on the street, or combine patient numbers with false provider numbers to file fake claims with insurers.

63. The value of Plaintiff's and the Class members' PHI on the black market is considerable. Stolen PHI trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" Internet websites, making the information publicly available, for a substantial fee.

64. It can take patients years to spot healthcare identity or PHI theft, giving criminals plenty of time to exploit that information for as much cash as possible. That is exactly why medical data PHI is more desirable to criminals than credit card theft. Credit card or financial information theft can be spotted by banks early on, and accounts can be quickly frozen or cancelled once the fraud is detected, making credit card and financial data much less valuable to criminals than PHI.

65. Luxottica has disclosed and given access to the PHI of Plaintiff and class members for criminals to use in the conduct of criminal activity. Specifically, Luxottica has opened up, disclosed, and exposed the contact information and PHI of Plaintiff and class members to persons engaged in disruptive and unlawful business practices and tactics, including spam and "phishing" emails, robo-dialed calls, junk texts and faxes, other unwanted calls and communications, online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (*i.e.*, identity fraud), all using the stolen PHI.

66. In recognition of the value of PHI, today a growing number of legitimate companies are developing business models that center on giving consumers a choice on whether or not they themselves wish to monetize (*i.e.*, sell or rent) their "scrubbed" (*i.e.*, designed to be anonymous) health data. There are numerous startups that have built platforms to offer pay-to-access

---

value/#:~:text=Stolen%20health%20credentials%20can%20go,a%20cyber%20crime%20protection%20company (last visited November 25, 2020). Dark web monitoring is a commercially available service which, at a minimum, Luxottica can and should perform (or hire a third-party expert to perform).

information to researchers from universities, medical institutes, and pharmaceutical companies—and that allow consumers such as Plaintiff and class members to monetize their own PHI and turn a profit on it if they so choose.

67. Consumers who are customers of these startups receive compensation for allowing access to information such as that which was stolen in the Data Breaches, only anonymized or scrubbed.[35] By way of the Data Breaches, Luxottica has compromised not only Plaintiff's and class Members' privacy, but also a substantial portion of the value of their PHI that is being misused and monetized by cyber-criminals.

68. Luxottica's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for patient and consumer privacy, and has exposed the PII and PHI of Plaintiff and class members to cyber-criminals.

69. PII also has significant monetary value in part because criminals continue their efforts to obtain this data.[36] In other words, if any additional breach of sensitive data did not have incremental value to criminals, one would expect to see a reduction in criminal efforts to obtain such additional data over time. Instead, just the opposite has occurred. For example, the Identity Theft Resource Center reported 1,473 data breaches in 2019, which represents a 17 percent increase from the total number of breaches reported in 2018.[37]

70. The value of PII is key to unlocking many parts of the financial sector for consumers. Whether someone can obtain a mortgage, credit card, business loan, tax return, or even

---

[35]Depending on their health and demographics, users of CoverUS can generate the equivalent of $100 to $1,000 a month if they monetize their PHI. People with illnesses and special conditions that are of particular interest to researchers can earn even more money. Fast Company, "*Can This App That Lets You Sell Your Health Data Cut Your Health Costs*" by Ben Schiller, January 4, 2018.

[36]*Data Breaches Rise as Cybercriminals Continue to Outwit IT*, CIO Magazine (Sept. 28, 2014), available at http://www.cio.com/article/2686167/data-breach/data-breaches-rise-as-cybercriminals-continue-to-outwit-it.html (last visited November 25, 2020).

[37]*2019 End-of-Year Data Breach Report* (2019), Identity Theft Resource Center, *available at* https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last visited November 25, 2020).

apply for a job depends on the integrity of their PII. Similarly, the businesses that request (or require) consumers to share their PII as part of a commercial transaction do so with the expectation that its integrity has not been compromised.

71. Luxottica recognizes the value of PII, as its possession and processing of PII allows it to advance its own commercial or economic interests. Luxottica annually receives for the business's commercial purposes or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers.

72. Annual monetary losses for victims of identity theft are in the billions of dollars. In 2017, fraudsters stole $16.8 billion from consumers in the United States, which includes $5.1 billion stolen through bank account take-overs.[38]

73. The annual cost of identity theft is even higher. McAfee and the Center for Strategic and International Studies estimates that the likely annual cost to the global economy from cybercrime is $445 billion a year.[39]

74. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, in addition to the irreparable damage that may result from the theft of PII, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[40]

75. Even before the occurrence of identity theft, victims may spend valuable time and suffer from the emotional toll of a data breach. Plaintiff has spent at least one hour responding to

[38]Javelin, *2018 Identity fraud: Fraud Enters A New Era of Complexity*, available at https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity (last visited November 25, 2020).
[39]Insurance Information Institute, *Facts + Statistics: Identity theft and cybercrime*, available at https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (last visited November 25, 2020).
[40]U.S. Department of Justice, *Victims of Identity Theft, 2014* (Revised November 13, 2017), available at http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited November 25, 2020).

the Data Breach after receiving notice from Luxottica, including by conducting independent online research regarding the scope of the breach and monitoring his credit score. He will continue to expend time reviewing account statements and any correspondence from insurers and healthcare providers to guard against medical fraud.

76. The impact of identity theft can have ripple effects, which can adversely affect the future financial trajectories of victims' lives. For example, the Identity Theft Resource Center reports that respondents to their surveys in 2013-2016 described that the identity theft they experienced affected their ability to get credit cards and obtain loans, such as student loans or mortgages.[41] For some victims, this could mean the difference between going to college or not, becoming a homeowner or not, or having to take out a high interest payday loan versus a lower-interest loan.

77. In a recent survey conducted by the Medical Identity Fraud Alliance (MIFA), a healthcare industry trade group, 52 percent of victims said their information was used to obtain government benefits like Medicare or Medicaid.[42] And 59 percent had their identity used to obtain healthcare, while 56 percent said a scammer parlayed their data into prescription drugs or medical equipment.[43] This is all the type of injury and harm, including actual fraud, Luxottica knows full well has been reported to it as being suffered by Plaintiff and class Members, and is directly traceable to the Data Breach. This harm is not merely just possible or certainly impending, it has actually happened and is ongoing, and Plaintiff and all class Members are in imminent and immediate danger of being further subjected to this injury.

[41] Identity Theft Resource Center, *Identity Theft: The Aftermath 2017*, available at https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf (last visited November 25, 2020).
[42] https://securityintelligence.com/protect-what-you-collect-keep-protected-health-information-secure/ (last visited November 24, 2020).
[43] *Id.*

78. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances;
- 37.1% reported an inability to concentrate / lack of focus;
- 28.7% reported they were unable to go to work because of physical symptoms;
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues); and
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[44]

79. It is no wonder, then, that identity theft exacts a severe emotional toll on its victims. The 2017 Identity Theft Resource Center survey[45] evidences the emotional suffering experienced by victims of identity theft:

- 75% of respondents reported feeling severely distressed;
- 67% reported anxiety;
- 66% reported feelings of fear related to personal financial safety;
- 37% reported fearing for the financial safety of family members;
- 24% reported fear for their physical safety;
- 15.2% reported a relationship ended or was severely and negatively impacted by the identity theft; and
- 7% reported feeling suicidal.

80. There may also be a significant time lag between when PII is stolen and when it is actually misused. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen

[44] *Id.*
[45] *Id.*

> data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[46]

81. The risk of identity theft is particularly acute where detailed personal information is stolen, such as the PII that was compromised in the Data Breach.

82. As the result of the Data Breach, Plaintiff and class members have suffered or will suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. identity theft and fraud resulting from theft of their PII;
b. costs associated with the detection and prevention of identity theft and unauthorized use of their online accounts, including financial accounts;
c. losing the inherent value of their PII;
d. losing the value of Luxottica's explicit and implicit promises of adequate data security;
e. costs associated with purchasing credit monitoring and identity theft protection services;
f. unauthorized access to and misuse of their online accounts;
g. unauthorized access to and misuse of their private health information;
h. unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;
i. lowered credit scores resulting from credit inquiries following fraudulent activities;
j. costs associated with time spent and the loss of productivity or enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future

[46]U.S. Government Accountability Office, *Report to Congressional Requesters* (June 2007), http://www.gao.gov/new.items/d07737.pdf (last visited November 25, 2020).

consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, addressing other varied instances of identity theft – such as credit cards, bank accounts, loans, government benefits, and other services procured using the stolen PII, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, updating login information for online accounts sharing the same login credentials as were compromised in the Data Breach, and the stress, nuisance, and annoyance of dealing with the repercussions of the Data Breach;

k. the continued imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being in the possession of one or more unauthorized third parties; and

l. continued risk of exposure to hackers and thieves of their PII, which remains in Luxottica's possession and is subject to further breaches so long as Luxottica fails to undertake appropriate and adequate measures to protect Plaintiff and class members.

83. Additionally, Plaintiff and class members place significant value in data security. According to a recent survey conducted by cyber-security company FireEye, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that has better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.[47] Indeed, Plaintiff has taken steps to protect himself from identity theft and fraud. He does not share PII or PHI through websites he knows to be unsecure and he periodically monitors his credit report (such reviewing of his credit score having increased in frequency following his receipt of notice of the Data Breach). Before the

[47]FireEye, *Beyond the Bottom Line: The Real Cost of Data Breaches* (May 11, 2016), https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html (last visited November 25, 2020).

Data Breach, these measures were successful – Plaintiff had not previously suffered identity theft and, to his knowledge, had not been the victim of a data breach compromising his PHI.

84. The cost of hosting or processing Patients' PII on or through Luxottica's computer data and storage systems includes things such as the actual cost of the servers and employee hours needed to process said transactions. One component of the cost of using these services is the explicit and implicit promises Luxottica made to protect Patients' PII. Because of the value consumers place on data privacy and security, companies with robust data security practices can command higher prices than those who do not. Indeed, if consumers did not value their data security and privacy, companies like Luxottica would have no reason to tout their data security efforts to their actual and potential customers.

85. Had the victims of the Data Breach, including Plaintiff, known the truth about Luxottica's data security practices—that Luxottica would not adequately protect and store their data—they would have demanded that their eye healthcare provider not store or process their PII through Luxottica's computer data and storage systems and would not have paid for, or would have paid less for, services at retailers using Luxottica's systems, including Target Optical

86. Plaintiff and class members are at an imminent risk of fraud, criminal misuse of their PII, and identity theft for years to come as result of the data breach and Luxottica's deceptive and unconscionable conduct.

CLASS ACTION ALLEGATIONS

87. Pursuant to Federal Rule of Civil Procedure 23(b)(1), (b)(2) and (b)(3), Plaintiff seeks certification of the following Class:

88. **Class:** All consumers in the United States whose PII was compromised in the Data Breach.

89. The Class asserts claims against Luxottica for negligence (Count 1), negligence per se (Count 2), declaratory judgment (Count 3), breach of confidence (Count 4), breach of express

contract (Count 5), breach of implied contract (Count 6), and violation of Ohio's Consumer Sales Practices Act (Count 7).

90. Pursuant to Federal Rules of Civil Procedure 23(b)(1), (b)(2) and (b)(3), Plaintiff seeks certification of California state claims in the alternative to the Class claims, as well as certification of claims for violations of the California Unfair Competition Law (Count 8), the California Customer Records Act (Count 9) and the California Consumer Privacy Act (Count 10), on behalf of a subclass of California residents, defined as follows:

91. **California Subclass**: All consumers in California whose PII was compromised in the Data Breach.

92. The Class and California Subclass are collectively referred to herein as the "Class."

93. Excluded from the Class are any Luxottica eye healthcare providers, centers, doctors, or retailers, Luxottica itself, any entity in which Luxottica has a controlling interest, and Luxottica's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class are any judicial officer presiding over this matter, members of their immediate family, members of their judicial staff, and any judge sitting in the presiding court system who may hear an appeal of any judgment entered.

94. **Risk of Inconsistent or Varying Adjudications. Fed. R. Civ. P. 23(b)(1).** As the proposed Class members include hundreds of thousands of Patients, there is significant risk of inconsistent or varying adjudications with respect to individual Class members that would establish incompatible standards of conduct for Luxottica. For example, injunctive relief may be entered in multiple cases, but the ordered relief may vary, causing Luxottica to have to choose between differing means of upgrading its data security infrastructure and choosing the court order with which it will comply. Class action status is also warranted because prosecution of separate actions by the members of the Class would create a risk of adjudications with respect to individual members of the Class that, as a practical matter, would be dispositive of the interests of other

members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

95. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. Luxottica has admitted that hundreds of thousands of Patients across the country were affected by the Data Breach.

96. **Commonality and Predominance. Fed. R. Civ. P. 23(a)(2) and (b)(3).** This action involves common questions of law and fact that predominate over any questions affecting individual Class members. The common questions include, but are not limited to:

a. Whether Luxottica knew or should have known that its computer and data storage systems were vulnerable to attack;

b. Whether Luxottica omitted or misrepresented material facts regarding the security of its computer and data storage systems and their inability to protect vast amounts of sensitive data, including Plaintiff's and Class members' PII;

c. Whether Luxottica failed to take adequate and reasonable measures to ensure such computer and data systems were protected;

d. Whether Luxottica failed to take available steps to prevent and stop the Data Breach from happening;

e. Whether Luxottica failed to disclose the material facts that it did not have adequate computer systems and security practices to safeguard PII;

f. Whether Luxottica owed duties to Plaintiff and Class members to protect their PII;

g. Whether Luxottica owed a duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class members;

h. Whether Luxottica breached its duties to protect the PII of Plaintiff and Class members by failing to provide adequate data security;

i. Whether Luxottica breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class members;

j. Whether Luxottica's failure to secure Plaintiff's and Class members' PII in the manner alleged violated federal, state and local laws, or industry standards;

k. Whether Luxottica was negligent, reckless or intentionally indifferent in its representations to Plaintiff and Class members concerning its security protocols;

l. Whether Luxottica was negligent in making misrepresentations to Plaintiff and Class members;

m. Whether Luxottica was negligent in establishing, implementing, and following security protocols;

n. Whether the Plaintiff's and Class members' PII was compromised and exposed as a result of the Data Breach and the extent of that compromise and exposure;

o. Whether Luxottica's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach, resulting in the unauthorized access to and/or theft of Plaintiff's and Class members' PII;

p. Whether Luxottica has a contractual obligation to use reasonable security measures and whether it complied with such contractual obligation;

q. Whether Luxottica's conduct amounted to violations of Ohio's consumer protection statutes;

r. Whether Luxottica's conduct amounted to violations of California consumer protection and data breach statutes;

s. Whether, as a result of Luxottica's conduct, Plaintiff and Class members face a significant threat of harm and/or have already suffered harm, and, if so, the appropriate measure of damages to which they are entitled;

t. Whether, as a result of Luxottica's conduct, Plaintiff and Class members are entitled to injunctive, equitable, declaratory and/or other relief, and, if so, the nature of such relief;

u. Whether Plaintiff and Class members are entitled to compensatory damages;

v. Whether the Plaintiff and Class members are entitled to punitive damages; and

w. Whether the Plaintiff and Class members are entitled to statutory damages.

97. **Typicality. Fed. R. Civ. P. 23(a)(3).** Plaintiff's claims are typical of other Class members' claims because Plaintiff and Class members were subjected to the same allegedly unlawful conduct and damaged in the same way.

98. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiff is an adequate representative of the Class. Plaintiff is a member of the Class and the California Subclass. Plaintiff has no conflicts of interest with the Class. Plaintiff's counsel are competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation and consumer protection claims. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the interests of the Class.

99. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual Plaintiff and Class members may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Class members are relatively small compared to the burden and expense required to individually litigate their claims against Luxottica, and thus, individual litigation to redress Luxottica's wrongful conduct would be impracticable. Individual litigation by each Class member would also strain the court system. Moreover, individual litigation creates the potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

100. **Injunctive and Declaratory Relief. Fed. R. Civ. P. 23(b)(2).** Class certification is also appropriate under Rule 23(b)(2). Luxottica, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole. Moreover, Luxottica continues to maintain its inadequate security practices, retains possession of Plaintiff's and the Class members' PII, and has not been forced to change its practices or to relinquish PII by nature of other civil suits or government enforcement actions, thus making injunctive and declaratory relief a live issue and appropriate to the Class as a whole.

* * *

Count 1

NEGLIGENCE

Against Luxottica on Behalf of Plaintiff and the Class or, Alternatively, on Behalf of Plaintiff and the California Subclass

101. Plaintiff repeats the allegations in paragraphs 1 – 100 in this Complaint, as if fully alleged herein.

102. Luxottica, in offering optometry and vision services to its customers and the ability to schedule appointments through the Scheduling Application, knew that Plaintiff and Class members' sensitive PII would be stored or processed by Luxottica computer and data storage systems, including on the Scheduling Application. Luxottica, in fact, stored and/or processed this PII through and on its computer systems and/or databases, utilizing the Scheduling Application.

103. By collecting, storing, and using this data, Luxottica had a duty of care to Plaintiff and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting this PII in Luxottica's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing Luxottica's security systems and data storage architecture to ensure that Plaintiff's and Class members' PII was adequately secured and

protected; (b) implementing processes that would detect an unauthorized breach of Luxottica's security systems and data storage architecture in a timely manner; (c) timely acting on all warnings and alerts, including public information, regarding Luxottica's security vulnerabilities and potential compromise of the PII of Plaintiff and Class members; (d) maintaining data security measures consistent with industry standards and applicable state and federal law; and (e) timely and adequately informing Plaintiff and Class members if and when a data breach occurred notwithstanding undertaking (a) through (d) above.

104. Luxottica had common law duties to prevent foreseeable harm to Plaintiff and Class members. These duties existed because Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices in Luxottica's affirmative collection of Patients' PII. In fact, not only was it foreseeable that Plaintiff and Class members would be harmed by the failure to protect their PII because hackers routinely attempt to steal such information and use it for nefarious purposes, Luxottica knew that it was more likely than not Plaintiff and other Class members would be harmed by such theft.

105. Luxottica had a duty to monitor, supervise, control, or otherwise provide oversight to safeguard the PII that was collected, stored, and processed by Luxottica computer and data storage systems.

106. Luxottica's duties to use reasonable security measures also arose as a result of the special relationship that existed between Luxottica, on the one hand, and Plaintiff and Class members, on the other hand. The special relationship arose because Plaintiff and class members entrusted Luxottica with their PII by virtue of their participation in the optometry and vision services offered by Luxottica. Luxottica alone could have ensured that its security systems and data storage architecture were sufficient to prevent or minimize the Data Breach.

107. Luxottica's duties to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair

practice of failing to use reasonable measures to protect PII. Various FTC publications and data security breach orders further form the basis of Luxottica's duties. In addition, individual states have enacted statutes based upon the FTC Act, including Ohio's Consumer Sales Practices Act and California's Unfair Competition Law, that also created a duty.

108. Luxottica's duties to use reasonable data security measures also arose under the California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.100, *et seq.*, which imposes a "duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information."

109. Luxottica's duties to use reasonable data security measures also arose under the California Consumer Records Acts ("CCRA"), Cal. Civ. Code §§ 1798.80, *et seq.*, which requires that any business that "owns, licenses, or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure."

110. The harm that has occurred is the type of harm the FTC Act (and similar state statutes, including those of Ohio and California), and the CCPA and CCRA, were intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of Luxottica's failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class members.

111. Luxottica knew or should have known that its computer systems and data storage architecture were vulnerable to unauthorized access and targeting by hackers for the purpose of stealing and misusing confidential PII.

112. Luxottica knew or should have known that a breach of its systems and data storage architecture would inflict millions of dollars of damages upon Plaintiff and the Class, and Luxottica was therefore charged with a duty to adequately protect this critically sensitive information.

113. Luxottica breached the duties it owed to Plaintiff and Class members described above and thus, was negligent. Luxottica breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiff and Class members; (b) detect the breach while it was ongoing; (c) maintain security systems consistent with industry standards; (d) and timely informing its Patients of the fact and extent of the Data Breach. These failures constituted both violations of the FTC Act (and similar state statutes), as well as a breach of duties owed to Plaintiff and Class members under the common law.

114. Luxottica also failed to exercise reasonable care and breached the duties it owed Plaintiff and Class members when it provided the thieves and/or subsequent unauthorized recipients of the stolen information with additional time and cover to further purloin and re-sell the stolen PII belonging to Plaintiff and the Class; provided the thieves and the purchasers and/or other subsequent unauthorized recipients with an opportunity to directly defraud Plaintiff and the Class; and failed to promptly notify Plaintiff and Class members of the fact that their PII was compromised and in imminent jeopardy of falling further into the hands of cyber criminals.

115. But for Luxottica's wrongful and negligent breach of its duties owed to Plaintiff and Class members, their PII would not have been compromised.

116. As a direct and proximate result of Luxottica's negligence, Plaintiff and Class members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach not fully disclosed by Luxottica, reviewing bank

statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

Count 2

NEGELIGENCE PER SE

Against Luxottica on Behalf of Plaintiff and the Class

117. Plaintiff repeats the allegations in paragraphs 1 – 100 in this Complaint, as if fully alleged herein, and assert this claim in the alternative to their negligence claim to the extent necessary.

118. Pursuant to the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, Luxottica had a duty to provide fair and adequate computer systems and data security to safeguard the PII of Plaintiffs and Class Members.

119. The FTC Act prohibits "unfair . . . practices in or affecting commerce," which the FTC has interpreted to include businesses' failure to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Luxottica's duty in this regard. In addition, individual states have enacted statutes based upon the FTC Act, including Ohio's Consumer Sales Practices Act and California's Unfair Competition Law, that also created a duty.

120. Luxottica's duties to use reasonable data security measures also arose under the CCPA, Cal. Civ. Code § 1798.100, *et seq.*, which imposes a "duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information."

121. Luxottica's duties to use reasonable data security measures also arose under the CCRA, Cal. Civ. Code §§ 1798.80, *et seq.*, which requires that any business that "owns, licenses, or maintains Personal Information about a California resident shall implement and maintain

reasonable security procedures and practices appropriate to the nature of the information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure."

122. Luxottica solicited, gathered, and stored PII of Plaintiff and the Class members to facilitate transactions which affect commerce.

123. Luxottica violated the FTC Act (and similar state statutes, including Ohio's Consumer Sales Practices Act and California's Unfair Competition law), as well as the CCPA and the CCRA, by failing to use reasonable measures to protect PII of Plaintiff and the Class members and not complying with applicable industry standards, as described herein. Luxottica's conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach on Luxottica's systems.

124. Luxottica's violation of the FTC Act (and similar state statutes, including the Ohio Consumer Sales Practices Act and California's Unfair Competition Law), as well as its violations of the CCPA and CCRA, constitutes negligence per se.

125. Plaintiff and the Class members are within the class of persons that the FTC Act and similar state statutes were intended to protect. Plaintiff and the California Subclass members are within the class of persons that the CCPA and CCRA were intended to protect.

126. The harm that occurred as a result of the breach is the type of harm the FTC Act and similar state statutes, as well as the CCPA and CCRA, were intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures caused the same harm as that suffered by Plaintiff and the Class members.

127. As a direct and proximate result of Luxottica's negligence per se, Plaintiff and the Class members have suffered, and continue to suffer, damages arising from the breach as described herein and as will be proven at trial.

128. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and

economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach not fully disclosed by Luxottica, reviewing bank statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

Count 3

DECLARATORY JUDGMENT

Against Luxottica on Behalf of Plaintiff and the Class or, Alternatively, on Behalf of Plaintiff and the California Subclass

129. Plaintiff repeats the allegations in paragraphs 1 – 100 in this Complaint, as if fully alleged herein.

130. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, the Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

131. An actual controversy has arisen in the wake of the Data Breach regarding Luxottica's present and prospective common law and other duties to reasonably safeguard its users' PII, and whether Luxottica is currently maintaining data security measures adequate to protect Plaintiff and Class members from further data breaches that compromise their PII. Plaintiff and Class members remain at imminent risk that further compromises of their PII will occur in the future. This is true even if they are not actively using Luxottica's products or services.

132. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Luxottica continues to owe a legal duty to secure users' PII and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes;

b. Luxottica continues to breach this legal duty by failing to employ reasonable measures to secure Plaintiff and Class members' PII.

133. The Court also should issue corresponding prospective injunctive relief pursuant to 28 U.S.C. §2202, requiring Luxottica to employ adequate security practices consistent with law and industry standards to protect its users' PII.

134. If an injunction is not issued, Plaintiff and Class members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach of Luxottica. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Plaintiff and Class members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

135. The hardship to Plaintiff and Class members if an injunction does not issue exceeds the hardship to Luxottica if an injunction is issued. Among other things, if another data breach occurs at Luxottica, Plaintiff and Class members will likely be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Luxottica of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Luxottica has a pre-existing legal obligation to employ such measures.

136. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Luxottica, thus eliminating additional injuries that would result to Plaintiff, Class members, and the hundreds of thousands of Luxottica Patients whose PII would be further compromised.

Count 4

BREACH OF CONFIDENCE

Against Luxottica on Behalf of Plaintiff and the Class or, Alternatively, on behalf of Plaintiff and the California Subclass

137. Plaintiff repeats the allegations in paragraphs 1 – 100 in this Complaint, as if fully alleged herein.

138. At all times during Plaintiff's and Class members' interactions with Luxottica, Luxottica was fully aware of the confidential and sensitive nature of Plaintiff's and Class members' PII.

139. As alleged herein and above, Luxottica's relationship with Plaintiff and Class members was governed by terms and expectations that Plaintiff's and Class members' PII would be collected, stored, and protected in confidence, and would not be disclosed to the public or any unauthorized third parties.

140. Plaintiff and Class members provided their respective PII, which was both confidential and novel, to Luxottica with the explicit and implicit understandings that Luxottica would protect and not permit their PII to be disseminated to the public or any unauthorized parties.

141. Plaintiff and Class members also provided their respective PII to Luxottica with the explicit and implicit understandings that Luxottica would take precautions to protect the PII from unauthorized disclosure, such as following basic principles of encryption and information security practices.

142. Luxottica voluntarily received in confidence Plaintiff's and Class members' PII with the understanding that PII was confidential and novel and, as such, would not be disclosed or disseminated to the public or any unauthorized third parties.

143. Due to Luxottica's failure to prevent, detect, and avoid the Data Breach from occurring by following best information security practices to secure Plaintiff's and Class members' PII, Luxottica caused Plaintiff's and Class members' PII to be disclosed and misappropriated to

the public and unauthorized third parties beyond Plaintiff's and Class members' confidence, and without their express permission.

144. But for Luxottica's disclosure of Plaintiff's and Class members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and/or used by unauthorized third parties. The Data Breach was the direct and legal cause of the theft of Plaintiff's and Class members' PII, as well as the resulting damages.

145. The injury and harm Plaintiff and Class members suffered was the reasonably foreseeable result of Luxottica's unauthorized disclosure of Plaintiff's and Class members' PII. Luxottica knew its computer systems and technologies for accepting, securing, and storing Plaintiff's and Class members' PII had serious security vulnerabilities because Luxottica failed to observe even basic information security practices or correct known security vulnerabilities.

146. As a direct and proximate result of Luxottica's breaches of confidence, Plaintiff and Class members have been injured and were damaged as discussed herein and as will be proven at trial.

147. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach not fully disclosed by Luxottica, reviewing bank statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

Count 5

BREACH OF EXPRESS CONTRACT

Against Luxottica on Behalf of Plaintiff and the Class or, Alternatively, on behalf of Plaintiff and the California Subclass

148. Plaintiff repeats the allegations in paragraphs 1 – 100 in this Complaint, as if fully alleged herein, and assert this claim in the alternative to their breach of implied contract claim to the extent necessary.

149. Luxottica's Privacy Policy is an agreement between Luxottica and consumers who purchase products or services from it. Plaintiff and Class members entered into this valid and enforceable express contract with Luxottica.

150. The Privacy Policy details how Luxottica will both protect and use the PII provided by users of Luxottica's products and services, including PII stored on or processed through Luxottica's databases and systems that was provided to its retail and affiliated stores and dispensaries.

151. The Privacy Policy provides detailed information about what types of PII will be shared and with what entities. It further promises that, "[t]he security of your personal information is important to us. When you enter sensitive information (such as credit card number and/or social security number) on our registration or order forms, we encrypt that information using secure socket layer technology (SSL)."

152. The Privacy Policy further states that Luxottica, "follow[s] generally accepted industry standards to protect the personal information submitted to us, both during transmission and once we receive it."

153. The HIPAA Notice, which is incorporated into the Privacy Policy, further specifies that if Luxottica "discover[s] that your health information has been breached (for example, disclosed to or acquired by an unauthorized person, stolen, lost, or otherwise used or disclosed in violation of applicable privacy law) and the privacy or security of the information has been

compromised, we must notify you of the breach without unreasonable delay and in no event later than 60 days following our discovery of the breach."

154. Plaintiff and Class members on the one hand and Luxottica on the other formed a contract pursuant to the Privacy Policy when Plaintiff and Class members used Luxottica products and services. The clear or manifest intent of Luxottica and Plaintiff and Class members to provide benefits to Plaintiff and Class members through the protection of their PII that was stored or processed by Luxottica in accordance with the terms of the Privacy Policy is evidenced by references in the Privacy Policy to its applicability to Plaintiff and Class members' PII, including in those portions of the Privacy Policy referenced in Paragraphs 21 through 27 of this Complaint.

155. Luxottica breached the Privacy Policy (and incorporated HIPAA Notice) contract, to the detriment of Plaintiff and Class members, by failing to protect their PII. Specifically, Luxottica (1) failed to use reasonable measures to protect that information; (2) disclosed that information to unauthorized third parties, in violation of the agreement; and (3) failed to notify Plaintiff and class members of the Data Breach within 60 days, in violation of the agreement.

156. As a direct result of Luxottica's breach of contract, Plaintiff and the Class have suffered injury, have been damaged as described herein and as will be proven at trial, and are entitled to damages in an amount to be proven at trial.

157. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach not fully disclosed by Luxottica, reviewing bank statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost

benefit of their bargains and overcharges for services; and other economic and non-economic harm.

Count 6

BREACH OF IMPLIED CONTRACT

Against Luxottica on Behalf of Plaintiff and the Class or, Alternatively, on behalf of Plaintiff and the California Subclass

158. Plaintiff repeats the allegations in paragraphs 1 – 100 in this Complaint, as if fully alleged herein, and assert this claim in the alternative to their breach of express contract claim to the extent necessary.

159. Luxottica invited Patients, including Plaintiff and the Class Members, to use its Scheduling Application in order to receive eye healthcare treatment and related products and services. As consideration for the treatments and related products and services Luxottica was to provide, Plaintiff and Class members provided their PII to Luxottica. When Plaintiff and Class members provided their PII to Luxottica, they entered into implied contracts by which Luxottica agreed to protect their PII and only use it solely to provide eye healthcare treatment and related products and services. As part of the offer, Luxottica would safeguard the PII using reasonable or industry-standard means.

160. Accordingly, Plaintiff and the Class members accepted Luxottica's offer to provide eye healthcare treatments and related products and services (for which Luxottica was compensated by Plaintiff and Class members) and provided Luxottica their PII by using the Scheduling Application, among other means. Plaintiff and Class members fully performed their obligations under the implied contracts with Luxottica. However, Luxottica breached the implied contracts by failing to safeguard Plaintiff's and Class members' PII.

161. The losses and damages Plaintiff and Class members sustained that are described herein were the direct and proximate result of Luxottica's breaches of its implied contracts with them. Additionally, because Plaintiff and Class members continue to be Patients of Luxottica's

eye healthcare providers, and because damages may not provide a complete remedy for the breaches alleged herein, Plaintiff and Class members are therefore entitled to specific performance of the contracts to ensure data security measures necessary to properly effectuate the contracts maintain the security of their PII from unlawful exposure.

162. Luxottica's conduct as alleged herein also violated the implied covenant of good faith and fair dealing inherent in every contract, and Luxottica is liable to Plaintiff and Class members for associated damages and specific performance.

Count 7

OHIO'S CONSUMER SALES PRACTICES ACT

Ohio Rev. Code & Prof. Code §§ 1345, et seq.

Against Luxottica on Behalf of Plaintiff and the Class

163. Plaintiff repeats the allegations in paragraphs 1 – 100 in this Complaint, as if fully alleged herein.

164. Luxottica is a "person" and "supplier" as defined by Ohio Rev. Code § 1345.01.

165. Plaintiff and Class members are "consumers" who were injured by Luxottica's engaging in unfair and deceptive trade practices in connection with a consumer transaction.

166. Luxottica engaged in unfair and deceptive acts and practices in connection with a consumer transaction, in violation of Ohio Rev. Code §§ 1345.02, including:

a. Luxottica represented that its goods, services, and intangibles had performance characteristics, uses, and benefits that it did not have, in violation of Ohio Rev. Code § 1345.02(B)(1); and

b. Luxottica represented that its goods, services, and intangibles were of a particular standard or quality when they were not, in violation of Ohio Rev. Code § 1345(B)(2).

167. Luxxotica engaged in unconscionable acts and practices in connection with a consumer transaction, in violation of Ohio Rev. Code § 1345.03, including:

a. Knowingly taking advantage of the inability of Plaintiff and the Class members to reasonably protect their interest because of their ignorance of the issues discussed herein (Ohio Rev. Code Ann. § 1345.03(B)(1)); and

b. Requiring Plaintiff and Class members to enter into a consumer transaction on terms that Defendant knew were substantially one-sided in favor of Defendant (Ohio Rev. Code Ann. § 1345.03(B)(5)).

168. Luxottica's unfair, deceptive, and unconscionable acts and practices include the following:

a. Luxottica failed to implement and maintain reasonable security measures to protect Plaintiff's and Class members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach.

b. Luxottica failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents in the healthcare sector. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiff and Class members whose PII has been compromised.

c. Luxottica's failure to implement and maintain reasonable security measures also was contrary to legislatively declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45.

d. Luxottica's failure to implement and maintain reasonable security measures also lead to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Luxottica's inadequate security, consumers could not have reasonably avoided the harms that Luxottica caused.

e. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff' and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

f. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class members' PII, including by implementing and maintaining reasonable security measures;

g. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' PII; and

i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

169. Luxottica's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Luxottica's data security and ability to protect the confidentiality of consumers' PII.

170. Luxottica intended to mislead Plaintiff and Class members and induce them to rely on its misrepresentations and omissions.

171. Had Luxottica disclosed to Plaintiff and Class members that its computer and data storage systems were not secure and, thus, vulnerable to attack, Luxottica would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Luxottica received, maintained, and compiled Plaintiff's and Class members' PII, as part of the services Luxottica provided and for which Plaintiff and Class members paid, without advising Plaintiff and Class members that Luxottica's data security practices were insufficient to maintain the safety and confidentiality of Plaintiff's and Class

members' PII. Accordingly, Plaintiff and Class members acted reasonably in relying on Luxottica's misrepresentations and omissions, the truth of which they could not have discovered.

172. Luxottica acted intentionally, knowingly, and maliciously to violate Ohio's Consumer Sales Practices Act, and recklessly disregarded Plaintiff's and Class members' rights. Past breaches within the healthcare industry (and directed towards its parent company) put Luxottica on notice that its security and privacy protections were inadequate.

173. Luxottica's conduct as alleged above constitutes an act or practice previously declared to be deceptive or unconscionable by rule adopted under division (B)(2) of section 1345.05 and previously determined by Ohio courts to violate Ohio's Consumer Sales Practices Act and was committed after the decisions containing these determinations were made available for public inspection under division (A)(3) of Ohio Rev. Code § 1345.05. The applicable rule and Ohio court opinions include, but are not limited to:

a. *State ex rel DeWine v. Uber Technologies*, PIF No. 3419

b. *State ex rel Yost v. Equifax Inc*., PIF No. 3502

c. *State ex rel Yost v. Premera Blue Cross*, PIF No. 3503

d. *In re Adobe Systems Inc*., PIF No. 3460

e. *In re Neiman Marcus Group*, PIF No. 3383

f. *In re Target Corp*., PIF No. 3326

174. As a direct and proximate result of Luxottica's unfair and deceptive acts and practices, Plaintiff and Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages as described herein and as will be proved at trial. These losses include the diminished value of Plaintiff's and Class members' PII. Because the integrity of Plaintiff's and Class members' PII is crucial to their future ability to engage in many aspects of commerce, including obtaining a mortgage, credit card, business loan, tax return, or even applying for a job, the diminishment of the integrity of that PII corresponds to a diminishment in value. In other words, Plaintiff and Class members have both a

present or future property interest diminished as a result of Luxottica's unfair and deceptive acts and practices.

175. Plaintiff and Class members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Luxottica's unfair and deceptive business practices or use of their PII; declaratory relief; reasonable attorneys' fees and costs under Ohio Revised Code § 1345.09; injunctive relief; and other appropriate equitable relief.

Count 8

CALIFORNIA'S UNFAIR COMPETITION LAW

Cal. Bus. & Prof. Code §§ 17200, et seq.

Against Luxottica on Behalf of Plaintiff and the California Subclass

176. Plaintiff repeats the allegations in paragraphs 1 – 100 in this Complaint, as if fully alleged herein.

177. Luxottica is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

178. Luxottica violated Cal. Bus. & Prof. Code §§ 17200, *et seq.* ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

179. Luxottica's unfair acts and practices include:

a. Luxottica failed to implement and maintain reasonable security measures to protect Plaintiff's and California Subclass members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach. Luxottica failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents in the healthcare sector. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiff and California Subclass members whose PII has been compromised.

b. Luxottica's failure to implement and maintain reasonable security measures also was contrary to legislatively declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45, California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 *et seq.*, and California's Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq.

c. Luxottica's failure to implement and maintain reasonable security measures also lead to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Luxottica's inadequate security, consumers could not have reasonably avoided the harms that Luxottica caused.

d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

180. Luxottica has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, California's Consumer Privacy Act, Cal. Civ. Code §§ 1798.100, *et seq.*, and California common law.

181. Luxottica's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and California Subclass members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents in the healthcare sector, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff' and California Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.*, and California's Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 *et seq.*, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and California Subclass members' PII, including by implementing and maintaining reasonable security measures

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.*; and California's Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 *et seq.*

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and California Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45; California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.*; and California's Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 *et seq.*

182. Luxottica's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Luxottica's data security and ability to protect the confidentiality of consumers' PII.

183. Luxottica intended to mislead Plaintiff and California Subclass members and induce them to rely on its misrepresentations and omissions.

184. Had Luxottica disclosed to Plaintiff and California Subclass members that its computer and data storage systems were not secure and, thus, vulnerable to attack, Luxottica would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Luxottica received, maintained, and compiled Plaintiff's and California Subclass members' PII, as part of the services Luxottica provided and for which Plaintiff and California Subclass members paid, without advising Plaintiff and California Subclass members that Luxottica's data security practices were insufficient to maintain the safety and confidentiality of Plaintiff's and California Subclass members' PII. Accordingly, Plaintiff and California Subclass members acted reasonably in relying on Luxottica's misrepresentations and omissions, the truth of which they could not have discovered.

185. Luxottica acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff's and California Subclass members' rights. Past breaches within the healthcare industry put Luxottica on notice that its security and privacy protections were inadequate.

186. As a direct and proximate result of Luxottica's unfair, unlawful, and fraudulent acts and practices, Plaintiff and California Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages as described herein and as will be proved at trial. These losses include the diminished value of Plaintiff's and California Subclass members' PII. Because the integrity of Plaintiff's and California Subclass members' PII is crucial to their future ability to engage in many aspects of commerce, including obtaining a mortgage, credit card, business loan, tax return, or even applying for a job, the diminishment of the integrity of that PII corresponds to a diminishment in value. In other words, Plaintiff and California Subclass members have both a present or future property interest diminished as a result of Luxottica's unfair, unlawful, and fraudulent acts and practices.

187. Plaintiff and California Subclass members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Luxottica's unfair, unlawful, and fraudulent business practices or use of their PII; declaratory relief; reasonable

attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

Count 9

CALIFORNIA CUSTOMER RECORDS ACT

Cal. Civ. Code §§ 1798.80, et seq.

Against Luxottica on Behalf of Plaintiff and the California Subclass

188. Plaintiff repeats the allegations in paragraphs 1 – 100 in this Complaint, as if fully alleged herein.

189. "[T]o ensure that Personal Information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure."

190. Luxottica is a business that maintains Personal Information, within the meaning of Cal. Civ. Code § 1798.81.5, about Plaintiff and California Subclass members.

191. Businesses that maintain computerized data that includes Personal Information are required to "notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82(b). Among other requirements, the security breach notification must include "the types of Personal Information that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82.

192. Luxottica is a business that maintains computerized data that includes Personal Information as defined by Cal. Civ. Code § 1798.80.

193. Plaintiff and California Subclass members' Personal Information includes Personal Information as covered by Cal. Civ. Code § 1798.82.

194. Because Luxottica reasonably believed that Plaintiff's and California Subclass members' Personal Information, including PHI, was acquired by unauthorized persons during the Data Breach, Luxottica had an obligation to disclose the Data Breach immediately following its discovery to the owners or licensees of the Personal Information (i.e., Plaintiff and the California Subclass), as mandated by Cal. Civ. Code § 1798.82. Indeed, Luxottica's own HIPAA Notice states that it would provide affected individuals with notice of a data breach regarding PHI.

195. By failing to disclose the Data Breach immediately following its discovery, Luxottica violated Cal. Civ. Code § 1798.82.

196. As a direct and proximate result of Luxottica's violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiff and California Subclass members suffered damages, as described above and as will be proven at trial.

197. Plaintiff and California Subclass members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

Count 10

CALIFORNIA CONSUMER PRIVACY ACT

Cal. Civ. Code §§ 1798.100 et seq.

Against Luxottica on Behalf of Plaintiff and the California Subclass

198. Plaintiff repeats the allegations in paragraphs 1 – 100 in this Complaint, as if fully alleged herein.

199. Plaintiff and California Subclass members are "consumer[s]" as that term is defined in Cal. Civ. Code. § 1798.140(g).

200. Luxottica is a "business" as that term is defined in Cal. Civ. Code. § 1798.140(c). As set forth above, Luxottica is a corporation organized or operated for the profit or financial benefit of its shareholders or other owners. Luxottica does business in the State of California. Luxottica collects consumers' (including Plaintiff's and California Subclass members') personal information and determines the purposes and means of the processing of this personal information (e.g., it designs the systems that process and store consumers' personal information). Luxottica

annually receives for the business's commercial purposes or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers.

201. Plaintiff's and California Subclass members' PII is "nonencrypted and nonredacted personal information" as that term is used in Cal. Civ. Code § 1798.150(a)(1). At a minimum, this PII included the individual's first name or first initial and last name, in combination with medical information and health insurance information. In some instances, the PII also included Social Security numbers, financial information, and unique identification numbers issued on government documents (e.g., driver's license numbers).

202. The Data Breach constitutes "an unauthorized access and exfiltration, theft, or disclosure" pursuant to Cal. Civ. Code § 1798.150(a)(1).

203. Luxottica had a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the Plaintiff's and California Subclass Members' PII to protect said PII.

204. Luxottica breached the duty it owed to Plaintiff and California Subclass Members described above. Luxottica breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiff and California Subclass Members; (b) detect the breach while it was ongoing; and (c) maintain security systems consistent with industry standards.

205. Luxottica's breach of the duty it owed to Plaintiff and California Subclass Members described above was the direct and proximate cause of the Data Breach. As a result, Plaintiff and California Subclass members suffered damages, as described above and as will be proven at trial.

206. Plaintiff seeks injunctive relief in the form of an order enjoining Luxottica from continuing the practices that constituted its breach of the duty owed to Plaintiffs and California Subclass as described above. Concurrently with the filing of this Complaint, Plaintiff is serving a letter of notice on Luxottica pursuant to Cal. Civ. Code § 1798.150(b) and anticipates amending this Complaint to seek statutory damages upon receipt of a written statement from Luxottica in response to that letter of notice.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all Class members proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Luxottica as follows:

1) For an Order certifying the Class and the California Subclass, as defined herein, and appointing Plaintiff and Plaintiff's counsel to represent the Class as alleged herein;
2) For injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class members, including but not limited to an order:
    a) Prohibiting Luxottica from engaging in the wrongful and unlawful acts described herein;
    b) Requiring Luxottica to protect, including through adequate encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;
    c) Requiring Luxottica to delete, destroy, and purge the PII of Plaintiff and Class members unless Luxottica can provide the Court a reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and the Class members;
    d) Requiring Luxottica to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class members' PII;
    e) Requiring Luxottica to engage independent third-party security auditors and internal personnel to run automated security monitoring;
    f) Requiring Luxottica to audit, test, and train its personnel regarding any new or modified procedures;
    g) Requiring Luxottica to segment data by, among other things, creating firewalls and access controls so that if one area of Luxottica's network is compromised, hackers cannot gain access to other portions of Luxottica's systems;

h) Requiring Luxottica to conduct regular database scanning and security checks;

i) Requiring Luxottica to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiff and Class members;

j) Requiring Luxottica to routinely and continually conduct internal training and education, at least annually, to inform security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

k) Requiring Luxottica to implement, maintain, regularly review, and revise as necessary, a threat management program designed to appropriately monitor Luxottica's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

l) Requiring Luxottica to meaningfully educate all Class members about the threats they face as a result of the loss of their PII to third parties, as well as the steps affected individuals must take to protect themselves;

m) Requiring Luxottica to implement logging and monitoring programs sufficient to track traffic to and from its servers, as well as programs sufficient to protect infiltration of its computer and data storage systems; and

n) Requiring Luxottica to provide ten years of identity theft and fraud protection services to Plaintiff and Class members.

3) For an award of compensatory, consequential, and general damages, including nominal damages, as allowed by law in an amount to be determined;

4) For an award of statutory damages and punitive damages, as allowed by law in an amount to be determined;

5) For an award of restitution or disgorgement, in an amount to be determined;

6) For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

7) For prejudgment interest on all amounts awarded; and

8) Such other and further relief as the Court may deem just and proper.

JURY DEMAND

Plaintiff, on behalf of himself and the Class of all others similarly situated, hereby demands a trial by jury on all issues so triable pursuant to Rule 38 of the Federal Rules of Civil Procedure.

Dated: December 4, 2020

Respectfully submitted,

/s/ Jeffrey S. Goldenberg
Jeffrey S. Goldenberg
GOLDENBERG SCHNEIDER, L.P.A.
4445 Lake Forest Drive, Suite 490
Cincinnati, OH 45242
Telephone: (513) 345-8297
Facsimile: (513) 345-8294
Email: jgoldenberg@gs-legal.com

Melissa S. Weiner*
Joseph C. Bourne*
PEARSON, SIMON & WARSHAW, LLP
800 LaSalle Avenue, Suite 2150
Minneapolis, Minnesota 55402
Telephone: (612) 389-0600
Facsimile: (612) 389-0610
Email: mweiner@pswlaw.com
jbourne@pswlaw.com

Hassan A. Zavareei*
Mark A. Clifford*
TYCKO & ZAVAREEI LLP
1828 L Street NW, Suite 1000
Washington, D.C. 20036
Telephone: (202) 973-0900
Facsimile: (202) 973-0950
Email: hzavareei@tzlegal.com
mclifford@tzlegal.com

Jeff Ostrow*
Jonathan M. Streisfeld*
Kristen Lake Cardoso*
KOPELOWITZ OSTROW
FERGUSON WEISELBERG GILBERT
1 West Las Olas Blvd., Suite 500
Fort Lauderdale, FL 33301

Telephone: (954) 525-4100
Facsimile: (954) 525-4300
Email: streisfeld@kolawyers.com
cardoso@kolawyers.com

Counsel for Plaintiff and the Proposed Class and California Subclass

**Pro Hac Vice Applications Forthcoming*